

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN**

In re Flagstar December 2021 Data
Security Incident Litigation

Case No. 4:22-cv-11385

Hon. Shalina D. Kumar

CONSOLIDATED CLASS ACTION COMPLAINT

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Rd., Ste. 200
Kansas City, Missouri 64112
siegel@stuevesiegel.com

John Yanchunis
MORGAN & MORGAN, P.A.
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
jyanchunis@ForThePeople.com

Interim Co-Lead Class Counsel

INTRODUCTION

1. Flagstar Bank is the second largest mortgage warehouse lender nationally, the eighth largest bank mortgage originator nationally, and the sixth largest sub-servicer of mortgage loans nationwide, serving over 1.5 million accounts with \$363 billion in unpaid principal balances. It collects vast troves of personal information from its customers and prospective customers and profits from that data through its own marketing efforts and by sharing sensitive customer information to third parties. Flagstar understands it has an enormous responsibility to protect the data it collects, and assures customers through its Privacy Policy that Flagstar is “committed to maintaining the security of the data you provide us,” and has “built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected.” Flagstar likewise assures customers that it has “firewalls and prevention systems that stop unauthorized access to our network and computers.” But as Flagstar admitted, it completely failed to meet these obligations and protect sensitive customer data. As a result, Flagstar suffered a data breach compromising the sensitive personal information of over 1.5 million former and current Flagstar customers—its second major data breach in a single year.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because this is a class action in

which the matter in controversy exceeds the sum or value of five million dollars (\$5,000,000.00), there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of States different from that of at least one Class Member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

3. The Court has personal jurisdiction over Flagstar because Flagstar is headquartered in this District and is authorized to and regularly conducts business in the State of Michigan. Flagstar sells, markets, and advertises its products and services to Plaintiffs and Class Members located in the State of Michigan and, therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

4. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because Flagstar has a principal place of business in this district; Flagstar transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this district.

DEFENDANT

5. Defendant Flagstar Bancorp, Inc. is a corporation formed in Michigan with its principal place of business located at 5151 Corporate Drive, Troy, Michigan 48098. Defendant Flagstar Bank, FSB is a Michigan-based, federally chartered stock

savings bank with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098 (collectively, “Defendant” or “Flagstar”).

PLAINTIFFS

6. Plaintiffs are individuals who, upon information and belief, had personally-identifiable information (“PII”)¹ exfiltrated and compromised and subsequently made available to other criminals on the dark web, in the data breach announced by Flagstar on June 17, 2022 (the “Data Breach”), and they bring this action on behalf of themselves and all those similarly situated both across the United States and within their State of residence. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only Flagstar (and the cyber criminals) have knowledge of what information was compromised for each individual Plaintiff, Plaintiffs reserve their right to supplement their allegations with additional facts and injuries as they are discovered.

7. Plaintiffs place significant value in the security of their PII. Plaintiffs agreed to entrust their sensitive PII to Flagstar with the understanding that Flagstar would keep their information secure and employ reasonable and adequate security

¹ PII is information that is used to confirm an individual’s identity and can include an individual’s name, Social Security number, driver’s license number, phone number, financial information, and other identifying information unique to an individual.

measures to ensure that it would not be compromised. If Plaintiffs had known of Flagstar's lax and totally inadequate security practices with respect to Plaintiffs' PII, they would not have done business with Flagstar, would not have applied for and/or consented to Flagstar's provision of services, would not have opened, used, or applied for Flagstar's services at the applicable rates and on the applicable terms, or would have paid less because of the diminished value of Flagstar's services.

CALIFORNIA

8. Plaintiff John Scott Smith is a resident of the State of California and is a former Flagstar customer. Mr. Smith was notified by Flagstar that his PII was compromised in the Data Breach. As a result of the breach, Mr. Smith has suffered fraud in the form of unauthorized attempted bank transfers across multiple banks and multiple accounts, including a fiduciary account Mr. Smith maintained as part of his business. As a result of this fraud, Mr. Smith spent significant time at his bank addressing the unauthorized activity and changing his account information at various financial institutions. Mr. Smith operates as part of Mr. Smith's business. Further, as a result of the breach, Mr. Smith continues to spend time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Mr. Smith has already suffered injury and remains at a present and continuing risk of harm.

9. Plaintiff Christopher P. Kennedy is a resident of the State of California and is a current Flagstar customer. Mr. Kennedy was notified by Flagstar that his PII was compromised in the Data Breach. As a result of the breach, Mr. Kennedy froze his credit accounts with the major bureaus. As a further result of the breach, Mr. Kennedy spent time researching ways to protect his PII, including reviewing FTC recommendations for victims of data breaches, and has meticulously logged the time and effort he has expended to protect his credit and bank accounts from fraud. As a result of the breach, Mr. Kennedy, among other things, spent time and effort contacting the Department of Motor Vehicles for the State of California, the FBI, the IRS, the Franchise Tax Board, the Lakewood Sheriff, and his various bank institutions about the breach. Prior to the breach, Mr. Kennedy purchased identity theft and credit monitoring services. As a result of the breach, Mr. Kennedy will need to continue paying for these services indefinitely to monitor his accounts and attempt to mitigate against harm. Given the highly-sensitive nature of the information stolen, Mr. Kennedy has already suffered injury and remains at a present and continuing risk of harm.

10. Plaintiff Erin Tallman is a resident of the State of California and a current Flagstar customer. Ms. Tallman was notified by Flagstar that her PII was compromised in the Data Breach. As a result of the breach, Ms. Tallman has experienced an increase in suspicious phishing spam calls, text messages, and

physical mail following the breach. As a result of the breach, Ms. Tallman has spent time and effort researching the breach and monitoring her accounts for fraudulent activity. As a further result of the breach, Ms. Tallman has spent time changing her passwords on her various financial accounts, and has cancelled Flagstar's ability to automatically withdraw her mortgage payments from her checking account. Prior to the breach, Ms. Tallman utilized credit monitoring services through Chase. As a result of the breach, Ms. Tallman will need to continue utilizing this service indefinitely in order to mitigate against harm. Given the highly-sensitive nature of the information stolen, Ms. Tallman has already suffered injury and remains at a present and continuing risk of harm.

11. Plaintiff Mark Wiedder is a resident of the State of California and a former Flagstar customer. Mr. Wiedder was notified by Flagstar that his PII was compromised in the Data Breach. Mr. Wiedder's PII, including his Security Number, was located on the dark web following the breach. As a result of the breach, Mr. Wiedder has experienced an increase in suspicious phishing spam calls, text messages, and emails following the breach. As a result of the breach, Mr. Wiedder has spent time and effort researching the breach and monitoring his accounts for fraudulent activity, including monitoring identity theft protection services from Experian and Kroll, and exploring additional credit monitoring and identity theft insurance options. Given the highly-sensitive nature of the information stolen, Mr.

Wiedder has already suffered injury and remains at a present and continuing risk of harm.

COLORADO

12. Plaintiff Michael McCarthy is a resident of the State of Colorado and a current Flagstar customer. Mr. McCarthy was notified by a third-party monitoring company that his PII was compromised in the Data Breach. As a result of the breach, Mr. McCarthy has experienced an increase in suspicious phishing spam text messages and emails following the breach. As a result of the breach, Mr. McCarthy has spent time and effort researching the breach and monitoring his accounts for fraudulent activity, including monitoring identity theft protection services provided by Kroll and AAA. Given the highly-sensitive nature of the information stolen, Mr. McCarthy has already suffered injury and remains at a present and continuing risk of harm.

FLORIDA

13. Plaintiff Rafael Hernandez is a resident of the State of Florida and a former Flagstar customer. Mr. Hernandez was notified by Flagstar that his PII was compromised in the Data Breach. As a result of the breach, Mr. Hernandez has spent time and effort researching the breach and monitoring his accounts for fraudulent activity. As a further result of the breach, Mr. Hernandez monitors his credit reports regularly for suspicious activity, and maintains an account with Credit Karma for

identity theft protection services that he reviews on a weekly basis. Given the highly-sensitive nature of the information stolen, Mr. Hernandez has already suffered injury and remains at a present and continuing risk of harm.

INDIANA

14. Plaintiff William Worton is a resident of the State of Indiana and a former Flagstar customer. Mr. Worton was notified by Flagstar that his PII was compromised in the Data Breach. As a result of the breach, Mr. Worton has spent time and effort researching the breach and monitoring his accounts for fraudulent activity. As a result of the breach, Mr. Worton contacted Flagstar regarding its offer of credit monitoring. As a further result of the breach, Mr. Worton purchased credit monitoring services from Credit Karma, and will need to continue paying for this service indefinitely to mitigate against harm. Given the highly-sensitive nature of the information stolen, Mr. Worton has already suffered injury and remains at a present and continuing risk of harm.

MICHIGAN

15. Plaintiff Hassan Nasrallah is a resident of the State of Michigan and a current Flagstar customer. Mr. Nasrallah was notified by Flagstar that his PII was compromised in the Data Breach. As a result of the data breach, Mr. Nasrallah has experienced significant identity theft in the form of unauthorized bank accounts, a brokerage account, a retirement account, and multiple credit cards opened in his

name. As a result of the data breach, Mr. Nasrallah also experienced identity theft in the form of unauthorized tax returns. Mr. Nasrallah has also experienced fraud in the form of several fraudulent credit inquiries, which have negatively impacted his credit score. In response to these and other fraudulent occurrences, Mr. Nasrallah has spent substantial time, effort, and funds to mitigate the damage, including contacting the police and the Social Security Administration, and placing a fraud alert on his credit report. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Mr. Nasrallah has already suffered injury and remains at a present and continuing risk of harm.

16. Plaintiff Nathan Silva is a resident of the State of Michigan and a former Flagstar customer. Mr. Silva was notified by Flagstar that his PII was compromised in the Data Breach. As a result of the breach, Mr. Silva has suffered identity theft and fraud in the form of multiple unauthorized withdrawals from his banking cards. Prior to the breach, Mr. Silva purchased multiple credit monitoring services. As a result of the breach, Mr. Silva will need to continue paying for the services indefinitely in order to mitigate against harm. As a result of the breach, Mr. Silva has spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Mr. Silva has already suffered injury and remains at a present and continuing risk of harm.

17. Plaintiff Laurie Ewing Scanlon is a resident of the State of Michigan and a former Flagstar customer. Ms. Scanlon was notified by Flagstar that her PII was compromised in the Data Breach. As a result of the breach, Ms. Scanlon has experienced an increase in suspicious phishing spam calls, text messages and emails following the breach. As a result of the breach, Ms. Scanlon has suffered identity theft and fraud in the form of unauthorized access to her bank account. As a result of this identity theft and fraud, Ms. Scanlon spent time and effort contacting her bank to resolve fraudulent charges on her account. As a result of the breach, Ms. Scanlon has spent time and effort monitoring her accounts and credit reports for fraudulent activity. Prior to the breach, Ms. Scanlon purchased credit monitoring services from Norton Lifelock for an annual fee. As a result of the breach, Ms. Scanlon will need to continue paying for the service indefinitely in order to mitigate against harm. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Ms. Scanlon has already suffered injury and remains at a present and continuing risk of harm.

MISSOURI

18. Plaintiff Everett Turner is a resident of the State of Missouri and is a current Flagstar customer. Mr. Turner was notified by Flagstar that his PII was compromised in the Data Breach. Following the breach, Mr. Turner's PII, including his Flagstar loan number and related data, were located on the dark web; also

following the breach, Mr. Turner was notified by a third-party monitoring company that his PII was located on the dark web. As a result of the breach, Mr. Turner has experienced an increase in suspicious mortgage-related solicitations. As a result of the breach, Mr. Turner froze his credit accounts, purchased temporary credit monitoring and identity theft protection services from My Fico, and contacted Flagstar for guidance on how to mitigate harm in response to the breach. As a further result of the breach, Mr. Turner has spent significant time and effort researching the breach and regularly monitors his accounts for fraudulent activity, including through credit monitoring and identity theft protection services provided by Credit Karma, Nerd Wallet, ID Watch Dog, and Credit Identity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Mr. Turner has already suffered injury and remains at a present and continuing risk of harm.

WASHINGTON

19. Plaintiff Allie McLaughlin is a resident of the State of Washington and is a current Flagstar customer. Ms. McLaughlin was notified that her PII was compromised in the Data Breach. As a result of the Data Breach, Ms. McLaughlin has spent time and effort researching the breach and monitoring her accounts and credit reports for fraudulent activity. Given the highly-sensitive nature of the

information stolen, Ms. McLaughlin has already suffered injury and remains at a present and continuing risk of harm.

STATEMENT OF FACTS

A. Flagstar Collects, Stores, and Profits from Customer Information, And Promises to Keep It Secure.

20. In 2022, Flagstar operated 150 branches in areas including Indiana, California, Wisconsin, and Ohio, and its mortgage divisions operated nationally through 82 retail locations.² Then one of the largest banks in the United States,³ Flagstar had total assets of over \$23.2 billion and generated annual revenues in excess of \$1.6 billion.

21. On December 1, 2022, Flagstar's operations grew exponentially due to New York Community Bancorp, Inc.'s acquisition of its operations.⁴ Now, Flagstar's mortgage division conducts its nationwide operations through a wholesale network of approximately 3,000 mortgage originators.⁵ While its regional

² *About Flagstar*, WWW.FLAGSTAR.COM, <https://www.flagstar.com/about-flagstar.html> (as of June 28, 2022).

³ Phil Muncaster, *US Bank Data Breach Impacts Over 1.5 Million Customer*, INFOSECURITY-MAGAZINE, <https://www.infosecurity-magazine.com/news/us-bank-data-breach-impacts-15/> (last visited June 16, 2023).

⁴ *Press Release: New York Community Bancorp, Inc. Completes Acquisition of Flagstar Bancorp, Inc.*, NEW YORK COMMUNITY BANCORP, INC., <https://ir.mynycb.com/news-and-events/news-releases/press-release-details/2022/NEW-YORK-COMMUNITY-BANCORP-INC.-COMPLETES-ACQUISITION-OF-FLAGSTAR-BANCORP-INC/default.aspx> (last visited June 15, 2023).

⁵ *About Flagstar*, WWW.FLAGSTAR.COM, <https://www.flagstar.com/about->

headquarters is in Troy, Michigan, Flagstar operates 435 branches nationwide, “including strong footholds in the Northeast and Midwest and exposure to high growth markets in the Southeast and West Coast.” As of March 31, 2023, Flagstar manages \$123.8 billion in assets, \$83.3 billion of loans, deposits of \$84.8 billion, and total stockholders’ equity of \$10.8 billion.⁶

22. Flagstar’s mortgage division is the eighth largest originator of residential mortgages for the 12-months ended March 31, 2023, and is the industry’s sixth largest sub-servicer of mortgage loans nationwide, serving 1.5 million accounts with \$363 billion in unpaid principal balances. Flagstar’s parent company is the second largest mortgage warehouse lender nationally based on total commitments.⁷ Flagstar is a publicly traded company organized and operated for the profit and financial benefit of its shareholders. In 2022, Flagstar had annual gross revenues of \$1.17 billion.

23. To run its business, Flagstar collects, maintains, and profits from the PII of millions of U.S. customers. PII is information that is used to confirm an individual’s identity and can include an individual’s name, Social Security number, driver’s license number, phone number, financial information, and other identifying information unique to an individual. Flagstar collects this PII from all customers and

flagstar.html (as of June 28, 2022) (last visited June 15, 2023).

⁶ *Id.*

⁷ *Id.*

maintains and profits from the PII regardless of whether a customer terminates their relationship with Flagstar. Flagstar maintains the PII of former customers for an indefinite period of time. This highly-sensitive PII is stored on centralized servers maintained by Flagstar.

24. Flagstar’s Privacy Policy is available on its website and provides customers with detailed promises regarding the treatment of their PII, including how Flagstar uses and shares customers’ data for its own benefit and profit.⁸ Flagstar explains that it collects customers’ PII when customers “[o]pen an account or apply for a loan,” “[d]eposit money or use your debit card,” or “[p]ay your bills.”⁹ Flagstar discloses that it also collects customers’ personal information “from others, such as credit bureaus, affiliates, or other companies.”¹⁰ The Privacy Policy explains that the “types of personal information” Flagstar collects and shares “depend on the product or service you have with us,” but can include “Social Security number and income,” “[c]redit history and credit scores;” and “[a]ccount balances and payment history.”¹¹ It further states: “When you are no longer our customer, we continue to share your information as described in this notice.”¹²

⁸ *About Your Privacy*, [WWW.FLAGSTAR.COM, about-
https://www.flagstar.com/content/dam/flagstar/pdfs/
flagstar/PrivacyPolicy.pdf](https://www.flagstar.com/content/dam/flagstar/pdfs/flagstar/PrivacyPolicy.pdf) (last visited June 16, 2023).

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

25. Flagstar represents that “[a]ll financial companies need to share customers’ personal information to run their everyday business.” Flagstar confirms that it shares its customers’ personal data “[f]or our marketing purposes—to offer our products and services to you,” “[f]or joint marketing with other financial companies,” and “[f]or our affiliates’ everyday business purposes—information about your transactions and experiences.”¹³

26. After listing the ways Flagstar benefits from tracking and targeting its customers through collecting and maintaining their valuable PII, Flagstar’s Privacy Policy pledges to them that their PII is secure, stating: “[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law,” and “[t]hese measures include computer safeguards and secured files and buildings.”¹⁴

27. Flagstar’s California Privacy Notice & Policy applicable to California residents provides further insight into how Flagstar profits from its customers’ PII.¹⁵ Flagstar explains that it collects customers’ PII (including Social Security numbers and names) from numerous categories of sources, including “[f]rom you,” “[f]rom your devices when you interact with our websites, mobile applications and systems,”

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *California Privacy Notice & Policy*, [WWW.FLAGSTAR.COM, https://www.flagstar.com/legal-disclaimers/ccpa-privacy-notice.html](https://www.flagstar.com/legal-disclaimers/ccpa-privacy-notice.html) (last visited June 16, 2023).

“[f]rom you when you apply for and receive products and services,” “[f]rom Flagstar employees when you interact with them and provide PI,” “[f]rom brokers, correspondents, appraisers, legal counsel, government-sponsored entities, investors, prior servicers, credit bureaus and other public records,” and “[f]rom beneficiaries, counterparties and other third parties related to a transaction.”¹⁶

28. Further, Flagstar reveals that it collects customers’ PII for wide-ranging business and commercial purposes, including “[t]o market and our products and services.”¹⁷ Flagstar likewise discloses that it shares its customers’ PII with several categories of third parties, and sells and/or shares customers PII to third parties for “cross-context behavioral advertising,” (e.g., targeting advertising) including to “provide personalized ads.”¹⁸

29. Along with its Privacy Policy, Flagstar maintains a “Fraud Information Center,” on its website, and agrees and promises that “Flagstar is committed to your financial security,”¹⁹ acknowledging that “[r]apid advances in technology and creative criminal minds [that] make fraud a potentially serious threat on a variety of fronts.”²⁰ In recognition of the highly sensitive nature of the information that it

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Fraud Information Center*, [WWW.FLAGSTAR.COM](http://www.flagstar.com), <https://www.flagstar.com/fraud-information-center.html> (last visited June 16, 2023).

²⁰ *Id.*

obtains from its customers, as well as the damages that can be inflicted on consumers if this information is in the hands of identity thieves, Flagstar commits to its clients that “[p]rotecting your finances is a top priority,” and warns them that “[s]ecuring your financial information is essential to protecting your finances.”²¹

30. “That’s why,” Flagstar represents, “we closely monitor all types of white-collar crime, including identity theft and the rapidly growing area of mortgage fraud.”²² Flagstar further promises its customers that they have “firewalls and prevention systems that stop unauthorized access to our network computers, plus secure network protocols that ensure connections between our offices, partners, and customers.”²³

31. Flagstar’s webpage dedicated to “Data Security and Customer Privacy,” reiterates that Flagstar has “built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected.”²⁴

B. Despite its Promises, Flagstar Admits it Failed to Protect Plaintiffs’ PII, And Then Compounds its Failure by Providing Late, Inadequate Notice to Those Impacted.

²¹ *Preventing Fraud*, WWW.FLAGSTAR.COM, <https://www.flagstar.com/fraud-information-center/preventing-fraud.html> (last visited June 16, 2023).

²² *Id.*

²³ *Id.*

²⁴ *Data Security and Customer Privacy*, WWW.FLAGSTAR.COM, <https://www.flagstar.com/esg/governance/data-security-and-customer-privacy.html> (last visited June 16, 2023).

32. At the same time Flagstar collected, stored, and profited from Plaintiffs' PII and was actively communicating to consumers that it was "ensur[ing] our data and customer privacy are well-protected," it suffered its second data breach in a single calendar year, exposing over 1.5 million individual's PII.

33. Between December 3 and December 4, 2021, cyber criminals infiltrated Flagstar's corporate network and accessed a treasure trove of highly sensitive customer information stored on its servers, including full names and Social Security numbers for 1.5 million customers.

34. It remains unclear exactly when Flagstar learned of the Data Breach. Flagstar did not publicly acknowledge the Data Breach until June 17, 2022, when it posted a press release on its website.²⁵

35. Flagstar's press release was woefully insufficient and unreasonably vague, providing consumers with no meaningful detail regarding the Data Breach—omitting any detail regarding the Data Breach's cause, scope, or impact; the timeline of the investigation into the breach; or the remedial measures taken to ensure customers' data security moving forward. Instead, Flagstar downplays the Data Breach in broad terms: "Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in

²⁵ *Customer Data Information Center*, [WWW.FLAGSTAR.COM](https://www.flagstar.com/customer-support/customer-data-information-center.html), <https://www.flagstar.com/customer-support/customer-data-information-center.html> (last visited June 15, 2023).

handling these types of incidents, and reported the matter to federal law enforcement. We continue to operate all services normally. Since then, we have taken several measures to toughen our information security. We now believe we have strengthened our cyber vulnerabilities in the future.”²⁶ Flagstar did not disclose when it learned of the Data Breach.

36. Instead, Flagstar claimed it “concluded an extensive forensic investigation and manual document review” on June 2, 2022.²⁷ Meaning, Flagstar learned of the Data Breach, conducted an extensive investigation, and conducted a manual document review *without* notifying any customers of the Data Breach. Even after Flagstar concluded its review six months after the Data Breach event, which ostensibly revealed that over 1.5 million customers’ PII were exfiltrated, it waited an *additional* fifteen days to disclose the Data Breach to its customers. Flagstar’s press release fails to disclose any other details of the Data Breach, including the type of information exposed or the method of exposure.

37. Based on information Flagstar submitted to the Office of the Maine Attorney General, the Data Breach affected 1,547,169 people in the United States and included Social Security numbers.²⁸ Flagstar’s submission to the Maine

²⁶ *Id.*

²⁷ *Id.*

²⁸ OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, <https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml> (last visited June 16, 2023).

Attorney General claims the Data Breach was “discovered” on June 2, 2022—calling into question the type of “extensive forensic investigation” and “manual document review” that could have been completed in a single day.

38. In recognition that Plaintiffs now face fraud and identity theft as a result of Flagstar’s failure to protect their PII, Flagstar press release mentions its customers can seek two years of credit monitoring and identity protection services through Kroll—woefully insufficient protection in light of the lifetime exposure to identity theft.

39. Similar in content to its dedicated webpage, the data breach notification letters Flagstar mailed to Data Breach victims provide little additional detail regarding what occurred.²⁹ Generously describing the Data Breach as a “recent” security incident, Flagstar states the Data Breach “involved unauthorized access to our network” but provides no details on who accessed the network, how they did so, or the type of PII potentially accessed. Flagstar further states that “[u]pon learning of the incident, we promptly activated our incident response plan” and “[a]fter an extensive forensic investigation and manual document review, we discovered on June 2, 2022 that certain impacted files containing your personal information were

²⁹ OFFICE OF THE MAINE ATTORNEY GENERAL, *Flagstar Standard Notification Letter*, <https://www.documentcloud.org/documents/22064071-flagstar-standard-notification-letter-06-17-2022?responsive=1&title=1> (last accessed June 16, 2023).

accessed and/or acquired from our network between December 3, 2021 and December 4, 2021.”

40. The letters offer empty assurances that Flagstar has “**no evidence that any of your information has been misused.**” Noticeably absent from the letters, however, is any effort to explain whether Flagstar made any attempt to investigate if its customers’ data had in fact been misused. In short, Flagstar’s self-serving statement about misuse is meaningless: Flagstar necessarily would not receive reports of PII misuse from its customers until *after* Flagstar notified victims that their PII had been stolen in the Data Breach; put differently, customers would not be able to trace identity theft or fraud to Flagstar’s Data Breach until Flagstar disclosed the Data Breach to them. Flagstar included this disingenuous and facially dubious statement in its letters to downplay the substantial fraud risk faced by the victims of its Data Breach.

41. Contrary to Flagstar’s statement that “[w]e have no evidence that any of your information has been misused,” gigabytes of Flagstar data files, including from Plaintiffs named herein, can be found on the dark web, including everything from mortgage applications, closing documents, bank statements, and even recordings of Flagstar employees’ collection calls—a collection of Flagstar’s customers’ PII far surpassing the name, address, and social security number Flagstar has admitted was taken.

42. Likewise, compromised credentials for numerous Flagstar Bank employees can also be found on the dark web, which is one potential vector from which the attack may have originated.

43. Notwithstanding, Flagstar admits that victims are at risk of harm by advising them, in response to the data breach, to take certain actions like monitoring their financial accounts and “placing a fraud alert and/or security freeze on your credit files” to “help protect your personal information.” Flagstar also offered victims two years of credit monitoring services “out of an abundance of caution.” Flagstar likewise directed its customers to visit [flagstar.com/protect](https://www.flagstar.com/protect) “for further ways you can help protect yourself[.]”

44. Ironically, Flagstar advises customers that they should “remain vigilant,” and if they “have reason to believe” their information is being misused, they should “promptly notify” their bank or financial institution, and should “promptly report” any fraudulent activity or “any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and the Federal Trade Commission (FTC)”³⁰—advice Flagstar failed to heed when it failed to disclose that over 1.5 million customers’ PII was exposed for over six months.

³⁰ *Customer Data Information Center*, [WWW.FLAGSTAR.COM, https://www.flagstar.com/customer-support/customer-data-information-center.html](https://www.flagstar.com/customer-support/customer-data-information-center.html) (last visited June 16, 2023).

45. As Flagstar admits, “[s]ecuring your financial information is essential to protecting your finances,”³¹ meaning immediate notice of exposed PII was crucial to protecting Plaintiffs’ and the Class Members’ finances. As then Illinois Attorney General Lisa Madigan aptly put it, “the second somebody gets your credit or debit card information, it can be a matter of hours or days until it’s sold on the black market and someone’s starting to make unauthorized transactions.”³² Yet, to date, Flagstar has provided no explanation for why (1) it delayed notifying customers about the Data Breach for over six months after the Data Breach occurred; (2) it chose to conduct an “extensive forensic investigation and manual document review” *before* notifying customers about the existence of the Data Breach; and (3) even after its “extensive forensic investigation and manual document review,” was completed, Flagstar again waited over two weeks to disclose the existence of the Data Breach to its customers. By deliberately delaying disclosure of the Data Breach for weeks if not months, and by downplaying the risk that victim’s PII would be misused by bad actors in its delinquent notice to customers, Flagstar compounded the harm suffered by Plaintiffs and Class Members and prevented victims from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

³¹ *Preventing Fraud*, WWW.FLAGSTAR.COM, <https://www.flagstar.com/fraud-information-center/preventing-fraud.html> (last visited June 16, 2023).

³² Phil Rosenthal, *Just assume your credit and debit cards were hacked*, CHICAGO TRIBUNE, <https://www.chicagotribune.com/business/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html> (last visited June 16, 2023).

C. The Data Breach was Flagstar's Second in a Single Year.

46. The Data Breach and resulting harm suffered by Plaintiffs and Class Members is directly attributable to Flagstar's security lapses and data mismanagement. Indeed, Flagstar is no stranger to cybersecurity incidents. Rather, the instant Data Breach is the second major incident to impact Flagstar and its customers in a year.

47. In January 2021, a notorious ransomware gang called "Clop" breached the servers of Flagstar's vendor, Accellion, which Flagstar used to send and receive sensitive documents with their partners and customers. Clop accessed the customer data of 1.48 million Flagstar employees and customers, including names, Social Security numbers, addresses, tax records, and phone number.

48. On March 5, 2021, Flagstar publicly confirmed that the PII of its customers was compromised in the Accellion data breach by releasing a statement on its website.

49. On its webpage dedicated to the Accellion breach, Flagstar provided scant detail regarding the breach:

Flagstar Bank Statement on Accellion Vulnerability

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021, that the platform had a vulnerability that was exploited by an unauthorized party. After Accellion informed us of the incident, Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of

Flagstar's information on the Accellion platform and that we are one of numerous Accellion clients who were impacted.

50. Flagstar also cautioned its customers:

Information Security Best Practices

We are aware that those responsible for this incident are in some cases contacting Flagstar customers by e-mail and by telephone. These are communications from unauthorized individuals responsible for the Accellion incident, and you should not respond to them. If you receive a suspicious message, please do not open attachments or click on links.

51. Like in the instant Data Breach, Flagstar offered impacted customers two years of Kroll identity monitoring.

52. After Flagstar began notifying victims of the Accellion data breach, the hacking group released screenshots of stolen personal data including Social Security numbers, names, addresses, phone numbers, and tax records—with a warning that it had stolen a lot more.

53. It has since been revealed that Clop exploited a vulnerability in Accellion's File Transfer Appliance ("FTA"), which was a twenty-year old "legacy" file transfer software purportedly designed and sold for large file transfers. The FTA was an obsolete legacy product that was nearing end-of-life, leaving it vulnerable to compromise and security incidents. Indeed, "[m]ultiple security experts...highlight that Accellion FTA is a 20-year-old application designed to allow an enterprise to securely transfer large files but nearing the end of life," and that "Accellion asked

its customers late last year to switch over to a new product it offers[.]”³³ Lawsuits filed post-breach alleged Flagstar failed to make the switch to a new product, and knowingly continued using FTA—exposing its customers’ PII to the risk of theft, identity theft, and fraud.

D. Flagstar Knew it Was a Prime Target for Cyberattacks.

54. High profile data breaches at industry-leading companies are notorious, including Equifax (147 million records, September 2017), Heartland Bank (130 million records, January 2008), Capital One Bank (100 million records, March 2019),³⁴ JPMorgan Chase (83 million records, October 2014), Experian (24 million records, August 2020), First American Financial (885 million records, May 2019), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), and Whisper (900 million records, March 2020). These

³³ Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC, (Feb. 24, 2021, 6:17am), <https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/> (last visited June 15, 2023).

³⁴ Capital One was assessed an \$80 million civil penalty by the Office of the Comptroller of the Currency (“OCC”) due to its “failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank’s failure to correct the deficiencies in a timely manner.” *OCC Assesses \$80 Million Civil Money Penalty Against Capital One*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Aug. 6, 2020), available at <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html> (last visited June 22, 2023).

represent a fraction of the data breaches affecting the United States and the financial services sector specifically.

55. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach incidents.³⁵ Conditions have only worsened since: Statista estimates that “[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]” and that “[i]n the first half of 2020, there were 540 reported data breaches.”³⁶

56. The financial sector, specifically, is one of the most targeted sectors for cyberattacks, given the highly-sensitive, and highly valuable, PII that financial institutions collect and store.³⁷ According to a 2019 Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report, of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number

³⁵ *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, STATISTA (Aug. 2020).

³⁶ *Id.*

³⁷ *For Financial Institutions, Cyberthreats Loom Large*, FORBES, <https://www.forbes.com/sites/forbesfinancecouncil/2022/03/09/for-financial-institutions-cyberthreats-loom-large/?sh=69dd96d82ddb> (last visited June 16, 2023).

of sensitive records being exposed exceeding 100 million. In fact, approximately 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.³⁸

57. According to Check Point, there were 703 reported cyberattacks attempts per week in 2021 within the industry: a 53% increase since 2020.³⁹ According to the Identity Theft Resource Center, the financial services sector accounted for 15.5% of data breaches in Q3 of 2021.⁴⁰ In the Fourth Quarter of 2021, there was an all-time peak in weekly cyber-attacks per organization, counting over 900 attacks per organization.⁴¹ According to the Verizon 2021 Data Breach Investigations Report, “96% [of] breaches in the financial services industry were

³⁸ *2019 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited June 26, 2023); *62% of breached data came from financial services in 2019*, CIO DIVE, <https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/> (last visited June 16, 2023); *Bitglass’ 2019 Financial Breach Report*, BITGLASS.

³⁹ *Check Point Research: Cyber Attacks Increased 50% Year Over Year*, CHECK POINT BLOG, <https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/> (last visited June 16, 2023).

⁴⁰ *If You’re a Victim of a Data Breach*, NORTHWEST BANK, <https://financialwellnesscenter.northwest.bank/family-finances/identity-protection/article/if-youre-a-victim-of-a-data-breach> (last visited June 16, 2023).

⁴¹ *Check Point Research: Cyber Attacks Increased 50% Year Over Year*, CHECK POINT BLOG, <https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/> (last visited June 16, 2023).

financially motivated.”⁴² Federal Reserve Chairman Jerome Powell “warned last year that cyberattacks are the No. 1 threat to the global financial system.”⁴³

58. Bloomberg described the financial services sector’s 2021 as an “unrelenting year of fighting off cyber threats,” and warned financial services providers “should expect more of the same or even worse.”⁴⁴ The Financial Services Information Sharing and Analysis Center’s (“FS-ISAC”) annual report on cyber threats cited in the article, predicts “current trends to continue and possible worsen over the next year,” stating cybersecurity is “no longer just a back-office cost.”⁴⁵ These increases are “due to several factors,” including the “rapid digitization of financial services, which accelerated during the pandemic,” and “increased entry points for cyber criminals to possibly exploit.”⁴⁶ Teresa Walsh, who leads FS-ISAC’s global intelligence office, described the financial sector as experiencing “a dizzying number of vulnerabilities.”

59. “Cap Gemini’s Top Trends in Banking 2022 declared cybersecurity is becoming a competitive differentiator for banks.”⁴⁷ Indeed, cyber security attacks

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Financial Firms Brace for More Cyber Threats After Trying 2021*, BLOOMBERG, <https://www.bloomberg.com/news/articles/2022-03-10/financial-firms-poised-for-worse-cyber-threats-after-trying-year> (last visited June 16, 2023).

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

aimed at the banking sector “keep rising in frequency and intensity due to their high potential for payout.”⁴⁸

60. Against this backdrop, Flagstar knew it was in the business of collecting, maintaining, and storing PII for millions of past and current customers. Flagstar knew, or reasonably should have known, that the millions of PII records it collected, maintained, and stored made it a prime target for cyberattacks. Thus, Flagstar knew, or reasonable should have known, of the importance of safeguarding the PII in its care. Flagstar acknowledges this fact on its own website, stating “[r]apid advances in technological and creative criminal minds make fraud a potentially serious threat on a variety of fronts.”⁴⁹ Likewise, Flagstar knew, or reasonable should have known, of the foreseeable consequences that would result should it fail to do so—including the significant costs to individual consumers.

E. Flagstar Failed to Comply with Federal Law, Regulatory Guidance, and Industry-Standard Cybersecurity Practices.

61. Flagstar’s data security failures are attributable to its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII.

⁴⁸ *Banking industry sees 1318% increase in ransomware attacks in 2021*, SECURITY MAGAZINE, <https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021> (last visited June 16, 2023).

⁴⁹ *See Preventing Fraud*, WWW.FLAGSTAR.COM, <https://www.flagstar.com/fraud-information-center/preventing-fraud.html> (last visited June 16, 2023).

62. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain PII to implement and maintain “reasonable security procedures and practices” and to protect PII from unauthorized access. California is one such state and requires that “[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure.” Cal. Civ. Code § 1798.81.5(b).

63. Flagstar also failed to comply with Federal Trade Commission (“FTC”) guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

64. The FTC recommends:

- limiting access to customer information to employees who have a business reason to see it;

- keeping customer information in encrypted files provides better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,
- monitoring activity logs for signs of unauthorized access to customer information.⁵⁰

65. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁵¹

66. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which established guidelines for fundamental data security principles and

⁵⁰ FEDERAL TRADE COMMISSION, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.

⁵¹ FEDERAL TRADE COMMISSION, *Start With Security* at 2, available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

practices for business.⁵² The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

67. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

68. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the

⁵² FEDERAL TRADE COMMISSION, *Protecting PII: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

71. Flagstar was fully aware of its obligation to implement and use reasonable measures to protect the PII of its customers, including the need to encrypt customer data on their computer networks, but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Flagstar's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

72. As a “financial institution,”⁵³ that collects nonpublic personal information,⁵⁴ Flagstar also failed to comply with the Gramm-Leach-Bliley Act (“GLBA”),⁵⁵ which imposes “an affirmative and continuing obligation” on all financial institutions to “respect the privacy of [their] customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” 15 U.S.C. § 6801. Consistent with that duty, financial institutions are required to establish appropriate safeguards “to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.” *Id.*

73. Flagstar also failed to comply with the Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b). The Safeguards Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards,

⁵³ The GLBA defines a financial institution as “any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956].” 15 U.S.C. § 6809(3)(A).

⁵⁴ As defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1).

⁵⁵ 15 U.S.C. §§ 6801.1, *et seq.*

including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control these risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

74. Further, in a ruling that took effect in May 2022, the Federal Deposit Insurance Corp. (FDIC), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve (together, the “agencies”) now require banks to notify their primary federal regulator within 36 hours of determining whether a “significant computer-security incident” could disrupt business or the stability of the financial sector, and requires banks to inform affected bank customers “as soon as possible,” recognizing cyberattacks targeting the financial services industry “have increased in

frequency and severity in recent years.”⁵⁶ Flagstar violated this ruling by delaying notifying its customers of the cyber-attack for six months after it occurred.

75. Flagstar was aware of its obligations to protect its customers’ PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers’ PII from unauthorized access. In this case, Flagstar was at all times fully aware of its obligation to protect the PII of Flagstar’s former and current customers. Flagstar was also aware of the significant repercussions if it failed to do so because Flagstar collected PII from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

76. Though limited detail is available on the Data Breach and how it occurred, Flagstar’s failure to safeguard its customers’ PII suggests failure to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and prevention.

⁵⁶ *Fed, FDIC, OCC approve 36-hour window for reporting cyberattacks*, BANKING DIVE, <https://www.bankingdive.com/news/36-hour-window-fed-fdic-occ-cybersecurity-technology-vendor/592275/> (last visited June 16, 2023); FEDERAL RESERVE, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, available at <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf> (last visited June 16, 2023).

F. The Impact of the Data Breach on Plaintiffs and Class Members.

77. Flagstar's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, Social Security numbers, account and loan numbers, etc.—cyber criminals can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and faced an imminent and continued risk of further injury for the remainder of their lives, including identity theft and related cybercrimes due to the Data Breach.

78. In fact, there is strong evidence that Plaintiffs' and Class Members' PII from the Flagstar Breach is circulating on the dark web. Identity protection services have alerted individual customers to the presence of their PII on the dark web.

79. It is no wonder Plaintiffs' stolen PII is circulating on the dark web, as it is highly valuable. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."⁵⁷

⁵⁷ A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

80. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

81. The U.S. Government Accountability Office determined that “stolen data may be held for up to a year or more before being used to commit identity theft,” and that “once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.”⁵⁸ Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiffs will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar’s Data Breach. In other words, Plaintiffs have been harmed by

⁵⁸ U.S. GOV’T ACCOUNTABILITY OFF., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm> (last visited June 16, 2023).

the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

82. Plaintiffs and Class Members have also realized harm in the lost or reduced value of their PII. Flagstar admits the PII compromised in the Breach is valuable. As discussed above, Flagstar collects, retains, and uses Plaintiffs' PII to increase profits. Plaintiffs' PII is not only valuable to Flagstar, but Plaintiffs also place value on their PII based on their understanding that their PII is a financial asset to companies that collect it.⁵⁹

83. Plaintiffs and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiffs' PII that was permitted without authorization by Flagstar. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

84. Moreover, Plaintiffs and Class Members value the privacy of this information and expect Flagstar to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Flagstar or

⁵⁹ See, e.g., *Ponemon Institute, LLC, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) available at <https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html> (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at \$55.70).

provided their PII had they known Flagstar did not implement reasonable security measures to protect their PII.⁶⁰ Customers reasonably expect that the payments they make for Flagstar's services incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiffs and Class Members did not receive the benefit of their bargain with Flagstar because they paid a value for services they expected but did not receive.

85. Given Flagstar's failure to protect Plaintiffs' and the Class Members' PII despite a data breach earlier that same year, Plaintiffs have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII remains in Flagstar's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

⁶⁰ FIREEYE, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), <https://www.fireeye.com/current-threats/cost-of-a-data-breach/wp-real-cost-data-breaches.html> (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

86. In sum, Plaintiffs and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the lost value of access to Plaintiffs' and Class Members' PII permitted by Flagstar; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; (vi) Flagstar's retention of profits attributable to Plaintiffs' and Class Members' PII that Flagstar failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to Flagstar for services purchased, as Plaintiffs reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case; and (x) nominal damages.

CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

87. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the “Nationwide Class” or the “Class”):

All natural persons residing in the United States whose PII was compromised in the Data Breach.

88. The Nationwide Class asserts claims against Flagstar for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), breach of confidence (Count 4), invasion of privacy—intrusion upon seclusion (Count 5), breach of express contract (Count 6), breach of implied contract (Count 7), and declaratory judgment (Count 8).

STATEWIDE SUBCLASSES

89. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 9 through 18), on behalf of a separate statewide Subclasses for California, Colorado, Indiana, Michigan, and Washington (the “Subclasses” or “Statewide Subclasses”), defined as follows:

All natural persons residing in [name of state or territory] whose PII was compromised in the Data Breach.

90. Excluded from the Nationwide Class and the Subclasses are Flagstar; its officers, directors, or employees; any entity in which Flagstar has a controlling interest; and any affiliate, legal representative, heir, or assign of Flagstar. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

91. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Flagstar has acknowledged that over 1.5 million individuals' PII has been compromised. Those individuals' names and addresses are available from Flagstar's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least hundreds of Class Members in each Subclass, making joinder of all Subclass Members impracticable.

92. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** As to each Class and Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include:

- a. Whether Flagstar had a duty to protect PII;
- b. Whether Flagstar failed to take reasonable and prudent security measures to ensure its systems were protected.
- c. Whether Flagstar failed to take available steps to prevent and stop the Breach from happening;
- d. Whether Flagstar knew or should have known that its computer and data storage systems were vulnerable to attack;
- e. Whether Flagstar was negligent in failing to implement reasonable and adequate security procedures and practices;
- f. Whether Flagstar's security measures to protect its systems were reasonable in light known legal requirements;
- g. Whether Flagstar's conduct constituted unfair or deceptive trade practices;
- h. Whether Flagstar violated state or federal law when it failed to implement reasonable security procedures and practices;
- i. Which security procedures and notification procedures Flagstar should be required to implement;
- j. Whether Flagstar has a contractual obligation to provide for the security of customer PII;
- k. Whether Flagstar has complied with any contractual obligations to protect customer PII;
- l. What security measures, if any, must be implemented by Flagstar to comply with its contractual obligations;
- m. Whether Flagstar violated state consumer protection laws in connection with the actions described herein;

- n. Whether Flagstar failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;
- o. Whether Flagstar's conduct resulted in or was the proximate cause of the loss of the PII of Plaintiffs and Class Members;
- p. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Flagstar's failure to reasonably protect their PII;
- q. Whether Flagstar should retain the money paid by Plaintiffs and Class Members to protect their PII, and the profits Flagstar generated using Plaintiffs' and Class Members' PII;
- r. Whether Flagstar should retain Plaintiffs' and Class Members' valuable PII; and,
- s. Whether Plaintiffs and Class Members are entitled to damages or injunctive relief.

93. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Class and Subclasses, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' PII was in Flagstar's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

94. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing

this matter against Flagstar to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

95. Predominance & Superiority: Federal Rule of Civil Procedure 23(b)(3). Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Flagstar, and thus, individual litigation to redress Flagstar's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the

court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

96. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Flagstar or would be dispositive of the interests of members of the proposed Class.

97. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Class and Subclasses consist of individuals who provided their PII to Flagstar. Class Membership can be determined using Flagstar's records.

98. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Flagstar, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

99. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. The common issues include:

- a. Whether Flagstar had a duty to protect PII;
- b. Whether Flagstar failed to take reasonable and prudent security measures to ensure its systems were protected.
- c. Whether Flagstar failed to take available steps to prevent and stop the Breach from happening;
- d. Whether Flagstar knew or should have known that its computer and data storage systems were vulnerable to attack;
- e. Whether Flagstar was negligent in failing to implement reasonable and adequate security procedures and practices;
- f. Whether Flagstar's security measures to protect its systems were reasonable in light known legal requirements;
- g. Whether Flagstar's conduct constituted unfair or deceptive trade practices;
- h. Whether Flagstar violated state or federal law when it failed to implement reasonable security procedures and practices;
- i. Which security procedures and notification procedures Flagstar should be required to implement;
- j. Whether Flagstar has a contractual obligation to provide for the security of customer PII;
- k. Whether Flagstar has complied with any contractual obligations to protect customer PII;

- l. What security measures, if any, must be implemented by Flagstar to comply with its contractual obligations;
- m. Whether Flagstar violated state consumer protection laws in connection with the actions described herein;
- n. Whether Flagstar failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

100. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

101. Flagstar required Plaintiffs and Class Members to provide their PII as a condition of receiving financial services. Flagstar collected and stored the data for purposes of providing financial services as well as for commercial gain.

102. Flagstar owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Flagstar's security systems to ensure that Plaintiffs' and Class Members' PII in Flagstar's possession was

adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

103. Flagstar's duty to use reasonable care arose from several sources, including but not limited to those described herein.

104. Flagstar had common law duties to prevent foreseeable harm to Plaintiffs and the Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by Flagstar's failure to protect their PII because cyber criminals routinely attempt to steal such information and use it for nefarious purposes, Flagstar knew that it was more likely than not Plaintiffs and other Class Members would be harmed if it allowed such a breach.

105. Flagstar's duty to use reasonable security measures also arose as a result of the special relationship that existed between Flagstar, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted Flagstar with their PII as part of the applications for services Flagstar offers as a major bank and mortgage company.

Flagstar alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

106. Flagstar's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Flagstar. Various FTC publications and data security breach orders further form the basis of Flagstar's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

107. Flagstar's duty also arose from Flagstar's unique position as one of the largest servicers of mortgage loans in the United States. As a financial institution, Flagstar holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiffs and Class Members. Because of its role as the sixth largest sub-servicer of mortgages nationwide, Flagstar was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Flagstar Data Breach.

108. Flagstar admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

109. With regard to network security, Flagstar further acknowledges that it has “built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected.”

110. Flagstar knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by cyber criminals for the purpose of stealing and misusing confidential PII.

111. Flagstar also had a duty to safeguard the PII of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require Flagstar to reasonably safeguard sensitive PII, as detailed herein.

112. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Flagstar’s misconduct.

113. Flagstar breached the duties it owed to Plaintiffs and Class Members described above and thus was negligent. Flagstar breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security

systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and the Class Members' PII in Flagstar's possession had been or was reasonably believed to have been, stolen or compromised.

114. But for Flagstar's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised and sold on the dark web.

115. Flagstar's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

116. Plaintiffs and Class Members were foreseeable victims of Flagstar's inadequate data security practices, and it was also foreseeable that Flagstar's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

117. As a direct and proximate result of Flagstar's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be

proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Flagstar; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT 2

NEGLIGENCE *PER SE*

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

118. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

119. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by companies such as Flagstar of failing to use reasonable measures to protect PII.

120. The FTC publications and orders also form the basis of Flagstar’s duty.

121. Flagstar violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Flagstar’s conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach involving a company as large as Flagstar, including, specifically, the damages that would result to Plaintiffs and Flagstar.

122. In addition, under state data security statutes, Flagstar had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs’ and Class Members’ PII.

123. Flagstar's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

124. Flagstar likewise violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by, among other things: (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured and accessible to unauthorized third-parties from the internet; (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system; (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; (d) failing to adequately (i) test and/or monitor the system were the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment; and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII of more than 1.5 million individuals with one or more non-affiliated third parties.

125. Flagstar's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes *negligence per se*.

126. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTC Act and the GLBA were intended to protect.

127. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

128. Flagstar breached its duties to Plaintiffs and Class Members under the FTC Act, state data security statutes, and the GLBA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

129. Plaintiffs and Class Members were foreseeable victims of Flagstar's violations of the FTC Act, state data security statutes, and the GLBA. Flagstar knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

130. But for Flagstar's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

131. As a direct and proximate result of Flagstar's negligence *per se*, Plaintiffs and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Flagstar; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 3

UNJUST ENRICHMENT

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

132. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

133. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Flagstar and that was ultimately stolen in the Flagstar Data Breach.

134. Flagstar was benefitted by the conferral upon it of the PII pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. Flagstar understood that it was in fact so benefitted.

135. Flagstar also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Flagstar maintaining the privacy and confidentiality of that PII.

136. But for Flagstar's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with Flagstar.

137. Flagstar admits that it uses the PII it collects for, among other things, "our marketing purposes—to offer our products and services to you," and "joint marketing with other financial companies[.]"

138. Because of its use of Plaintiffs' and Class Members' PII, Flagstar sold more services than it otherwise would have. Flagstar was unjustly enriched by profiting from the additional services it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

139. Flagstar also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

140. Flagstar also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiffs' and Class Members' PII.

141. It is inequitable for Flagstar to retain these benefits.

142. As a result of Flagstar's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), Flagstar has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

143. Flagstar's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive PII, while at the same time failing to

maintain that information secure from intrusion and theft by cyber criminals and identity thieves.

144. It is inequitable, unfair, and unjust for Flagstar to retain these wrongfully obtained benefits. Flagstar's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

145. The benefit conferred upon, received, and enjoyed by Flagstar was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Flagstar to retain the benefit.

146. Flagstar's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other damages as described herein.

147. Plaintiffs have no adequate remedy at law.

148. Flagstar is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Flagstar as a result of its wrongful conduct, including specifically: the value to Flagstar of the PII that was stolen in the Data Breach; the profits Flagstar received and is receiving from the use of that information; the amounts that Flagstar overcharged Plaintiffs and Class Members for use of Flagstar's services; and the amounts that Flagstar should

have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

COUNT 4

BREACH OF CONFIDENCE

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

149. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

150. Plaintiffs and Class Members maintained a confidential relationship with Flagstar whereby Flagstar undertook a duty not to disclose to unauthorized parties the PII provided by Plaintiffs and Class Members to Flagstar to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

151. Flagstar knew Plaintiffs' and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

152. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Flagstar failed to implement and maintain

reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

153. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

154. But for Flagstar's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Flagstar's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

155. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Flagstar's unauthorized disclosure of Plaintiffs' and Class Members' PII. Flagstar knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and Class Members' PII had serious security vulnerabilities because Flagstar failed to observe basic information security practices or correct known security vulnerabilities.

156. As a direct and proximate result of Flagstar's breach of confidence, Plaintiffs and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes,

fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Flagstar; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; lost benefit of their bargains and overcharges for services; nominal and general damages; and other economic and non-economic harm.

COUNT 5

INVASION OF PRIVACY—INTRUSION UPON SECLUSION

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

157. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

158. Plaintiffs and Class Members shared PII with Flagstar that Plaintiffs and Class Members wanted to remain private and non-public.

159. Plaintiffs and Class Members reasonably expected that the PII they shared with Flagstar would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

160. Flagstar intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party.

161. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Flagstar unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

- a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;
- b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;
- c. Failing to adequately secure their PII from disclosure to unauthorized persons; and
- d. Enabling the disclosures of their PII without consent.

162. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

163. Flagstar's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

164. As a direct and proximate result of Flagstar's invasions of privacy, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Flagstar; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 6

BREACH OF EXPRESS CONTRACT

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

165. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. For the purposes of this claim, Plaintiffs and Class Members shall mean natural persons who were current customers of Flagstar as of December 3, 2021.

166. Flagstar's Privacy Policy is an agreement between Flagstar and individuals who provided their PII to Flagstar, including Plaintiffs and Class Members.

167. Flagstar's represents that its Privacy Policy applies to information it collects about individuals who seek, apply for, or obtain Flagstar's financial products and services for personal, family, or household purposes.⁶¹

168. Flagstar's Privacy Notice stated at the time of the Data Breach that Flagstar "use[s] security measures that comply with federal law," and "[t]hese measures include computer safeguards and secured files and buildings," in order to "protect your personal information from unauthorized access and use."

⁶¹ <https://www.flagstar.com/legal-disclaimers/ccpa-privacy-notice.html> (last visited June 16, 2023).

169. Flagstar further agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: “[f]or our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus,” “[f]or our marketing purposes – to offer our products and services to you,” “[f]or joint marketing with other financial companies,” and “[f]or our affiliates’ everyday business purposes – information about your transactions and experiences.”

170. None of the enumerated circumstances involve sharing Plaintiffs or the Class Members’ PII with a criminal hacker.

171. Plaintiffs and Class Members on the one side and Flagstar on the other formed a contract when Plaintiffs and Class Members obtained products or services from Flagstar, or otherwise provided PII to Flagstar subject to its Privacy Policy.

172. Plaintiffs and Class Members fully performed their obligations under the contracts with Flagstar.

173. Flagstar breached its agreement with Plaintiffs and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

174. As a direct and proximate result of Flagstar’s breach of contract, Plaintiffs and Class Members have been injured and are entitled to damages in an

amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Flagstar; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 7

BREACH OF IMPLIED CONTRACT

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of
Plaintiffs and the Statewide Subclasses**

175. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

176. Plaintiffs and Class Members entered into an implied contract with Flagstar when they obtained services from Flagstar, or otherwise provided PII to Flagstar.

177. As part of these transactions, Flagstar agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or compromised.

178. Plaintiffs and Class Members entered into the implied contracts with reasonable expectation that Flagstar's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members understood that Flagstar would use part of the monies paid to Flagstar under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security practices.

179. Plaintiffs and Class Members would not have provided and entrusted their PII to Flagstar or would have paid less for Flagstar's services in the absence of the implied contract or implied terms between them and Flagstar. The safeguarding

of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

180. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Flagstar.

181. Flagstar breached its implied contracts with Plaintiffs and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

182. As a direct and proximate result of Flagstar's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost

value of the PII; lost value of access to their PII permitted by Flagstar; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 8

DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Class,
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

183. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

184. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

185. An actual controversy has arisen in the wake of the Flagstar Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Flagstar is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs continue to suffer

injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII stored by Flagstar.

186. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Flagstar continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, various state statutes, and the GLBA;
- b. Flagstar continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

187. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Flagstar. The risk of another such breach is real, immediate, and substantial. If another breach at Flagstar occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

188. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Flagstar if an injunction is issued. Among other things, if another massive data breach occurs at Flagstar, Plaintiffs will likely be subjected to

substantial identity theft and other damage. On the other hand, the cost to Flagstar of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Flagstar has a pre-existing legal obligation to employ such measures.

189. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Flagstar, thus eliminating the additional injuries that would result to Plaintiffs and the 1.5 million consumers whose confidential information would be further compromised.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 9

CALIFORNIA CONSUMER PRIVACY ACT (“CCPA”), Cal. Civ. Code §§ 1798.150, *et seq.*

190. The California Plaintiff(s) identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

191. Plaintiffs and the California Subclass Members are residents of California.

192. Flagstar is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over \$1.6 billion. Flagstar collects customers’ personal information as defined in Cal. Civ. Code § 1798.140.

193. Flagstar violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and the California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Flagstar's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

194. Flagstar has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and the California Subclass Members' PII. As detailed herein, Flagstar failed to do so.

195. As a direct and proximate result of Flagstar's acts, Plaintiffs' and the California Subclass Members' PII, including Social Security numbers and names, was subjected to unauthorized access and exfiltration, theft, or disclosure.

196. Plaintiffs and the California Subclass Members seek injunctive or other equitable relief to ensure Flagstar hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Flagstar continues to hold customers' PII, including Plaintiffs' and the California Subclass Members' PII. Plaintiffs and the California Subclass Members have an interest in ensuring that their PII is reasonably protected, and Flagstar has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

197. Pursuant to Cal. Civ. Code § 1798.150(b), Plaintiffs Wiedder and Smith mailed CCPA notice letters to Defendant's registered service agent on June 28, 2022 and June 30, 2022, respectively, detailing the specific provisions of the CCPA that Flagstar has and continues to violate. Flagstar did not cure within 30 days.

198. As described herein, an actual controversy has arisen and now exists as to whether Flagstar implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

199. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Flagstar and third parties with similar inadequate security measures.

200. Plaintiffs and the California Subclass seek statutory damages of between \$100 and \$750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT 10

**CALIFORNIA CUSTOMER RECORDS ACT,
Cal. Civ. Code §§ 1798.80, *et seq.***

201. The California Plaintiff(s) identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

202. “[T]o ensure that personal information about California residents is protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that “owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure.”

203. Flagstar is a business that owns, maintains, and licenses personal information (or “PII”), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and the California Subclass Members.

204. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other

requirements, the security breach notification must include “the types of PII that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

205. Flagstar is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

206. Plaintiffs’ and the California Subclass Members’ PII (e.g., Social Security numbers) includes PII covered by Cal. Civ. Code § 1798.82.

207. Because Flagstar reasonably believed that Plaintiffs’ and the California Subclass Members’ PII was acquired by unauthorized persons during the Flagstar Data Breach, Flagstar had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

208. Flagstar failed to fully disclose material information about the Data Breach in a timely and accurate fashion.

209. By failing to disclose the Data Breach in a timely and accurate fashion, Flagstar violated Cal. Civ. Code § 1798.82.

210. As a direct and proximate result of Flagstar’s violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and the California Subclass Members suffered damages, as described above.

211. Plaintiffs and the California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 11

**CALIFORNIA UNFAIR COMPETITION ACT,
Cal. Bus. & Prof. Code §§ 17200, *et seq.***

212. The California Plaintiff(s) identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

213. Flagstar is a “person” as defined by Cal. Bus. & Prof. Code §17201.

214. Flagstar violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

215. Flagstar’s “unfair” acts and practices include:

- a. Flagstar failed to implement and maintain reasonable security measures to protect Plaintiffs’ and the California Subclass Members’ PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.
- b. Flagstar failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass Members, whose PII has been compromised.

- c. Flagstar's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.
- d. Flagstar's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Flagstar's grossly inadequate security, they could not have reasonably avoided the harms that Flagstar caused.
- e. Flagstar engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

216. Flagstar has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); California's Consumers Legal Remedies Act, Cal. Civ.

Code §§ 1780, et seq.; the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; and California common law.

217. Flagstar's unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTC Act (15 U.S.C. § 45); and the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the California Subclass Members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; California's Consumer Privacy Act, Cal. Civ. Code § 1798.100; California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.* and 1798.81.5, which was a direct and proximate cause of the Data Breach.

218. Flagstar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Flagstar's data security and ability to protect the confidentiality of consumers' PII.

219. As a direct and proximate result of Flagstar's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and the California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Flagstar's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

220. Flagstar acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and the California Subclass Members' rights. Flagstar's past data breach put it on notice that its security and privacy protections were inadequate.

221. Plaintiffs and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Flagstar's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 12

**CALIFORNIA CONSUMER LEGAL REMEDIES ACT,
Cal. Civ. Code §§ 1750, *et seq.***

222. The California Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

223. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* (“CLRA”) is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

224. Flagstar is a “person” as defined by Civil Code §§ 1761(c) and 1770, and has provided “services” as defined by Civil Code §§ 1761(b) and 1770.

225. Plaintiff and the California Subclass are “consumers” as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

226. Flagstar’s acts and practices were intended to and did result in the sales of products and services to California Plaintiffs and the California Subclass Members in violation of Civil Code § 1770, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade when they were not;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

227. Flagstar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Flagstar's data security and ability to protect the confidentiality of consumers' PII.

228. Had Flagstar disclosed to California Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Flagstar would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Flagstar was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. Flagstar accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on

Flagstar's misrepresentations and omissions, the truth of which they could not have discovered.

229. Pursuant to Cal. Civ. Code § 1782(a), Plaintiffs Smith mailed a CLRA notice letter to Defendant's registered service agent on June 30, 2022 detailing the specific provisions of the CLRA that Flagstar has and continues to violate. Flagstar did not cure within 30 days.

230. As a direct and proximate result of Flagstar's violations of California Civil Code § 1770, California Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Flagstar's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

231. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 13

**COLORADO SECURITY BREACH NOTIFICATION ACT,
Colo. Rev. Stat. §§ 6-1-716, et seq.**

232. The Colorado Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

233. Defendant is a business that owns or licenses computerized data that includes PII as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

234. Plaintiff and Colorado Subclass Members’ PII (e.g., Social Security numbers) includes PII as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

235. Defendant is required to accurately notify Plaintiff and Colorado Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

236. Because Defendant was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

237. By failing to disclose the Defendant data breach in a timely and accurate manner, Defendant violated Colo. Rev. Stat. § 6-1-716(2).

238. As a direct and proximate result of Defendant's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass Members suffered damages, as described above.

239. Plaintiff and Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT 14

COLORADO CONSUMER PROTECTION ACT, Colo. Rev. Stat. §§ 6-1-101, *et seq.*

240. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

241. Defendant is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

242. Defendant engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

243. Plaintiff and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Defendant or successors in interest to actual consumers.

244. Defendant engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

- a. Making a false representation as to the characteristics of products and services;
- b. Representing that services are of a particular standard, quality, or grade, though Defendant knew or should have known that there were or another;
- c. Advertising services with intent not to sell them as advertised;
- d. Employing “bait and switch” advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and
- e. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

245. Defendant’s deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite

knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

246. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

247. Defendant intended to mislead Plaintiff and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.

248. Had Defendant disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

249. Defendant acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

250. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Colorado Subclass Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII, monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

251. Defendant's deceptive trade practices significantly impact the public, because many members of the public are actual or potential consumers of Defendant's services and the Defendant Data Breach affected hundreds of thousands of Americans, which include members of the Colorado Subclass.

252. Plaintiff and Colorado Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) \$500, or (c) three times actual damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 15

**VIOLATION OF THE INDIANA DECEPTIVE CONSUMER SALES ACT,
Ind. Code § 24-5-0.5**

253. The Indiana Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Indiana Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

254. The Indiana Deceptive Consumer Sales Act (“IDCSA”) “shall be liberally construed and applied to promote its purposes and policies,” which include “protect[ing] consumers from suppliers who commit deceptive and unconscionable sales acts.” Ind. Code § 24-5-0.5-1.

255. The IDCSA defines a “supplier” as “[a] seller, lessor, assignor, or other person who regularly engages in or solicits consumer transactions, including ... a manufacturer, wholesaler, or retailer, whether or not the person deals directly with the consumer.” *Id.* § 24-5-0.5-2(a)(3)(A).

256. Defendant is a “supplier” under the IDCSA.

257. The IDCSA defines an “incurable deceptive act” as “a deceptive act done by a supplier as part of a scheme, artifice, or device with intent to defraud or mislead.” *Id.* § 24-5-0.5-2(a)(8).

258. The IDCSA regulates the conduct of suppliers, as follows:

A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.

Id. § 24-5-0.5-3(a).

259. Defendant engaged in incurable deceptive acts under the IDCSA related to consumer transactions with Plaintiff and the Indiana Subclass, as follows:

- a. failing to implement adequate data security practices to safeguard PII;
- b. failing to encrypt the sensitive PII of Plaintiff and the Indiana Subclass, including their Social Security Numbers; and
- c. failing to make only authorized disclosures of current and former customers' PII;
- d. failing to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft; and
- e. failing to timely and accurately disclose the Data Breach to Plaintiff and the Indiana Subclass.

260. The IDCSA provides that “[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars (\$500), whichever is greater.” *Id.* § 24-5-0.5-4(a). Moreover, “[t]he court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (1) three (3)

times the actual damages of the consumer suffering the loss; or (2) one thousand dollars (\$1,000).” *Id.*

261. The IDCSA provides that a senior consumer, defined as “an individual who is at least sixty (60) years of age,” may recover treble damages for an incurable deceptive act. *Id.* §§ 24-5-0.5-2(a)(9), 24-5-0.5-4(i).

262. Plaintiff and the Indiana Subclass are entitled to and demand recovery of the maximum statutory damages available under the IDCSA.

263. Under IDCSA § 24-5-0.5-4(a), Plaintiff and the Indiana Subclass are entitled to and demand recovery of reasonable attorney fees.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 16

VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT, (Mich. Comp. Laws Ann. § 445.901 et seq.)

264. The Michigan Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

265. Plaintiff and the Michigan Subclass are “persons” as defined by Mich. Comp. Laws Ann. § 445.903(d).

266. Flagstar advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

267. Flagstar engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);
- b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);
- c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and
- d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

268. Flagstar's unfair, unconscionable, and deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect the PII of Plaintiff and the Michigan Subclass, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiff and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Rule, Regulation P, and the Safeguards Rule, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of the PII of Plaintiff and the Michigan Subclass, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiff and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Act, Regulation P, and the Safeguards Rule;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the PII of Plaintiff and the Michigan Subclass; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiff and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Act, Regulation P, and the Safeguards Rule.

269. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

270. Defendant intended to mislead Plaintiff and the Michigan Subclass and induce them to rely on its misrepresentations and omissions.

271. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded the rights of Plaintiff and the Michigan Subclass.

272. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff and the Michigan Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with

Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

273. Plaintiff and the Michigan Subclass seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, restitution, injunctive relief, and any other relief that is just and proper.

COUNT 17

WASHINGTON DATA BREACH NOTICE ACT,

Wash. Rev. Code §§ 19.255.010, *et seq.*

274. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

275. Flagstar is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Wash. Rev. Code § 19.255.010(1).

276. Plaintiff's and Washington Subclass Members' PII includes PII as defined by Wash. Rev. Code § 19.255.005(2) and covered under Wash. Rev. Code § 19.255.010(1).

277. Flagstar is required to accurately notify Plaintiff and Washington Subclass Members following discovery or notification of the breach of its data security system if PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(8).

278. Because Flagstar discovered a breach of its security system in which PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, Flagstar had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010, including by identifying in the notice the types of PII that were subject to the breach.

279. By failing to disclose the Flagstar data breach in a timely and accurate manner and failing to provide the information required, Flagstar violated Wash. Rev. Code § 19.255.010(1).

280. As a direct and proximate result of Flagstar violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass Members suffered damages, as described above.

281. Plaintiff and Washington Subclass Members seek relief under Wash. Rev. Code §§ 19.255.040(3)(a) and 19.255.040(3)(b), including actual damages and injunctive relief.

COUNT 18

WASHINGTON CONSUMER PROTECTION ACT,

Wash. Rev. Code §§ 19.86.020, *et seq.*

282. The Washington Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

283. Flagstar is a “person,” as defined by Wash. Rev. Code § 19.86.010(1).

284. Flagstar advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code § 19.86.010 (2).

285. Flagstar engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

286. Flagstar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Flagstar's data security and ability to protect the confidentiality of consumers' PII.

287. Flagstar acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights. Flagstar's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

288. Flagstar's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the many Washingtonians affected by the Flagstar Data Breach.

289. As a direct and proximate result of Flagstar's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described

herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Flagstar's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

290. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Flagstar, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead Interim Class Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Flagstar from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

- a. Prohibiting Flagstar from engaging in the wrongful and unlawful acts described herein;
- b. Requiring Flagstar to protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- c. Requiring Flagstar to delete, destroy and purge the PII of Plaintiffs and Class Members unless Flagstar can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- d. Requiring Flagstar to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;
- e. Requiring Flagstar to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Flagstar's systems on a periodic basis, and ordering Flagstar to promptly correct any problems or issues detected by such third-party security auditors;

- f. Requiring Flagstar to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- g. Requiring Flagstar to audit, test, and train their security personnel regarding any new or modified procedures;
- h. Requiring Flagstar to segment data by, among other things, creating firewalls and access controls so that if one area of Flagstar's network is compromised, cyber criminals cannot gain access to other portions of Flagstar's systems;
- i. Requiring Flagstar to conduct regular database scanning and securing checks;
- j. Requiring Flagstar to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII , as well as protecting the PII of Plaintiffs and Class Members;
- k. Requiring Flagstar to routinely and continually conduct internal training and education, at least annually, to inform internal

security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

- l. Requiring Flagstar to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Flagstar's policies, programs and systems for protecting PII;
- m. Requiring Flagstar to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Flagstar's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- n. Requiring Flagstar to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;
- o. Requiring Flagstar to implement logging and monitoring programs sufficient to track traffic to and from Flagstar servers; and

p. At Flagstar's expense, appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Flagstar's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

3. That the Court award Plaintiffs and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Flagstar as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiffs be granted the declaratory relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: June 23, 2023

Respectfully submitted,

/s/ Norman E. Siegel

Norman E. Siegel, MO #44378
Barrett J. Vahle, MO #56674
Jordan A. Kane, MO #71028
STUEVE SIEGEL HANSON LLP
460 Nichols Rd., Ste. 200
Kansas City, MO 64112
(816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
kane@stuevesiegel.com

Interim Co-Lead Class Counsel

/s/ David H. Fink

David H. Fink (P28235)
Nathan J. Fink (P75185)
Fink Bressack PLLC
38500 Woodward Avenue, Suite 350
Bloomfield Hills, Michigan 48304
Telephone: (248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

Interim Liaison Counsel

E. Powell Miller
The Miller Law Firm, P.C.
950 W. University Drive, Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
epm@millerlawpc.com

Danielle L. Perry
Mason LLP
5335 Wisconsin Avenue NW, Suite 640

/s/ John Yanchunis

John Yanchunis
Patrick Barthle
Morgan & Morgan Complex Litigation
Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 223-5505
jyanchunis@ForThePeople.com
Pbarthle@ForThePeople.com

Interim Co-Lead Class Counsel

Rachel K. Tack
Zimmerman Reed LLP
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400
rachel.tack@zimmermanreed.com

Michael Reese
Reese LLP
100 W. 93rd Street, 16th Floor

Washington, District of Columbia 20015
Telephone: (202) 429-2290
dperry@masonllp.com

New York, New York 10025
Telephone: (212) 594-5300
mreese@reesellp.com

Jamisen A. Etzel
Lynch Carpenter LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
jamisen@lcllp.com

Plaintiffs' Executive Committee